

CLAIM AMENDMENTS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1 1. (Currently Amended) A method for backing up data on a plurality of
2 computers connected via a network, comprising:
3 forming one or more partnerships between among the plurality of
4 computers such that each computer in a partnership commits under an
5 agreements to ~~help~~ store backup ~~the~~ data received from one or more of its
6 backup partners, whereby a first computer in each partnership assumes the
7 task of storing backup data received from one or more other computers in the
8 partnership and one or more of the other computers in the partnership assume
9 the task of storing backup data received from the first computer;
10 backing up data in accordance with ~~the~~ each agreements; and
11 periodically verifying that previously backed up data is being retained
12 by the computers committed to act as backup partners in accordance with ~~the~~
13 each agreements.

1 2. (Original) The method of claim 1, further comprising:
2 selecting potential backup partners from among the plurality computers
3 based on predetermined criteria.

1 3. (Original) The method of claim 1, further comprising:
2 negotiating the agreements between the plurality of computers based
3 on predetermined requirements, including backup requirements.

1 4. (Currently Amended) The method of claim 1, wherein the plurality of
2 computers ~~can~~ administer a distributed cooperative backing up of data in the
3 absence of central control.

1 5. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the data is encoded with an erasure code.

1 6. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the data is encoded with an error correction code.

1 7. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the data is encrypted.

1 8. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the data is encoded with an erasure code and then encrypted, the
3 encoding being for fault tolerance and the encryption being for data security.

1 9. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the data is compressed and then encoded with an erasure code.

1 10. (Withdrawn) The method of claim 9, wherein the compression is a
2 lossless data compression.

1 11. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the data is, in sequence, compressed, encoded with an erasure code
3 and encrypted.

1 12. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the method further comprises, in sequence:
3 performing data compression;
4 performing a first data encryption;
5 performing encoding with an erasure code; and
6 performing a second data encryption.

1 13. (Withdrawn) The method of claim 12, wherein the first encryption is for
2 data security and the second encryption is for preventing freeloading by any of
3 the backup partners, and wherein the encoding is for fault tolerance.

1 14. (Withdrawn) The method of claim 1, further comprising:
2 restoring data from the previously backed up data.

1 15. (Original) The method of claim 1, wherein each of the plurality of
2 computers has a storage, the storage being periodically scanned to find data to
3 be backed up and identify data previously backed up that no longer needs to be
4 backed up, the data to be backed up being retrieved from the storage for a next
5 periodic backup.

1 16. (Currently Amended) The method of claim 1, wherein the verifying that
2 previously backed up data is retained by the backup partners includes
3 monitoring the backup partners, and for any one of the backup partners being
4 monitored,
5 selecting a block of data stored at the monitored backup partner,
6 requesting the block of data from the monitored backup partner, and
7 receiving from the monitored backup partner and checking the block of
8 data to determine if the block of data represents a corresponding block of
9 previously backed up data.

1 17. (Original) The method of claim 16, wherein the block is selected
2 randomly.

1 18. (Currently Amended) The method of claim 16, wherein the block is
2 selected using a protocol to produce a number that corresponds to the selected
3 block and that is not controlled by any one backup partner individually.

1 19. (Original) The method of claim 18, wherein the protocol, being
2 performed by any computer of the plurality of computers, includes
3 sending by the computer to a monitored one of its backup partners a
4 hash value of a first random number,
5 receiving by the computer from the monitored one of its backup
6 partners a second random number,
7 sending by the computer to the monitored one of its backup partners
8 the first random number,
9 computing the number from the first and second random numbers by
10 both the computer and the monitored one of its backup partners.

1 20. (Original) The method of claim 1, further comprising:
2 selecting another computer connected via the network to be a new
3 backup partner if it is determined that a backup partner has reneged by not
4 retaining the previously backed up data;
5 negotiating and, if an agreement is reached, forming a partnership with
6 the other computer, accepting the other computer as the new backup partner.

1 21. (Original) The method of claim 20, wherein selecting another computer
2 to be the new backup partner includes
3 determining if there are sufficient backup partners for backing up the
4 data, and
5 searching for the other computer based on predetermined criteria
6 including one or both of geographic separation and system diversity.

1 22. (Original) The method of claim 20, wherein if after accepting the other
2 computer as the new backup partner it is determined that the backup partners
3 are insufficient in number for backing up the data, the selecting, negotiating
4 and forming backup partnership with yet another computer are repeated, the
5 determining, selecting, negotiating and forming backup partnership being
6 repeated until the number of backup partners is sufficient.

1 23. (Original) The method of claim 2, wherein selecting computers as
2 potential backup partners includes
3 determining if there are sufficient backup partners for backing up the
4 data, and
5 searching for computers based on the predetermined criteria that
6 includes one or both of geographic separation and system diversity.

1 24. (Original) The method of claim 3, wherein negotiating the agreements
2 includes, for any computer of the plurality of computers,
3 exchanging queries between the computer and computers selected as
4 its potential backup partners about each such computer's ability to satisfy the
5 predetermined requirements that include one or more of
6 predictable and suitable time schedule for being on-line,

7 suitable network bandwidth,
8 matching backup space requirements, and
9 backup track record.

1 25. (Original) The method of claim 24, wherein, the computer prefers to
2 partner with those of its potential backup partners that satisfy the
3 predetermined requirements.

1 26. (Original) The method of claim 24, wherein the suitable network
2 bandwidth is equal or larger than a predetermined threshold bandwidth and is
3 characterized by an average bandwidth that is larger than the predetermined
4 threshold bandwidth.

1 27. (Original) The method of claim 24, wherein the backup track record
2 includes not renegeing on a number of other backup partners that is greater than
3 a predetermined number.

1 28. (Original) The method of claim 1, wherein each of the backup partners
2 has a recent copy of a list of its backup partners' other backup partners.

1 29. (Withdrawn) The method of claim 1, wherein a user of each of the
2 plurality of computers can obtain a copy of a list containing identifiers and/or
3 identities of the backup partners associated therewith and an encryption key
4 under which the data is encrypted prior to being backed up.

1 30. (Original) The method of claim 1, wherein the agreements are
2 respectively negotiated between the plurality of computers such that in each
3 partnership each computer commits to avoid making or honoring data
4 restoration request for a predetermined commitment period that is longer than
5 a grace period, wherein the grace period for a backup partner of a computer
6 starts to run if it is determined that the backup partner has failed to respond to
7 such computer verifying that the backup partner is retaining the previously
8 backed up data or to prove to such computer that it is retaining the previously

9 backed up data, and wherein upon the grace period running out such computer
10 considers the backup partner to have reneged on its agreement.

1 31. (Withdrawn) The method of claim 7, wherein any encryption algorithm
2 can be suitably used for encrypting the data being backed up, including DES
3 (data encryption standard), RC4, RSA or other public-key encryption.

1 32. (Withdrawn) The method of claim 6, wherein the error correction code is
2 a Reed Solomon code.

1 33. (Withdrawn) The method of claim 5, wherein for a low degree of fault
2 tolerance the erasure code is $n+1$ -parity.

1 34. (Withdrawn) The method of claim 7, wherein after the encryption of the
2 data the encrypted data is divided into blocks and cryptographic checksums or
3 digital signature are added to each block before the blocks are sent each to a
4 particular one of the backup partners.

1 35. (Withdrawn) The method of claim 5, wherein the encoding with the
2 erasure code uses Tornado coding.

1 36. (Withdrawn) The method of claim 5, wherein the encoding with the
2 erasure code includes
3 dividing the data being backed up into blocks, and
4 adding redundancy to each of the blocks producing data objects with
5 actual data portions and redundant data portions, so that each one of the actual
6 data portions and redundant data portions is being backed up at a distinct one
7 of the backup partners.

1 37. (Withdrawn) The method of claim 1, further comprising:
2 dividing the data being backed up into blocks;
3 creating a hash value of each of the blocks using a key; and
4 correspondingly appending the hash values to their blocks before the
5 blocks are each sent to a distinct one of the backup partners.

1 38. (Withdrawn) The method of claim 37, wherein the hash values are later
2 used in periodically verifying that the previously backed up data is retained by
3 the backup partners and, if needed, that the previously backed up data being
4 retained is valid and can be used to restore lost data.

1 39. (Withdrawn) The method of claim 37, wherein the periodic verifying
2 includes
3 selecting and requesting a particular one of the data blocks that was
4 previously backed up,
5 retrieving the particular one of the data blocks and its associate hash
6 value,
7 computing a new hash value from the retrieved particular block using
8 the key, and
9 comparing the new hash value with the associated hash value to
10 determine if they are equal, equality indicating that the data block is retained
11 by the backup partner and is valid.

1 40. (Withdrawn) The method of claim 1, wherein the encoding includes
2 dividing the data being backed up into p groups of m blocks, each of the p
3 groups representing a vector of actual data and the m blocks in each of the p
4 groups representing m elements of the actual data vector; and adding
5 redundancy to each actual data vectors producing p codewords each being a
6 vector of $n=m+k$ elements, so that each one of the n elements is being backed
7 up at a distinct one of the backup partners.

1 41. (Withdrawn) The method of claim 14, wherein the restoring of data from
2 the previously backed up data includes
3 retrieving blocks of the previously backed up data from the backup
4 partners until sufficient blocks of the previously backed up data are available
5 for decoding,
6 checking, for each retrieved block of the previously backed up data, if
7 the retrieved block is valid and intact,

8 decoding all the retrieved blocks of the previously backed up data to
9 reconstruct the data originally backed up.

1 42. (Withdrawn) The method of claim 14, wherein the restoring of data from
2 the previously backed up data includes
3 retrieving previously backed up data from the backup partners until
4 sufficient previously backed up data is available for decoding,
5 decoding all the retrieved previously backed up data to reconstruct the
6 data originally backed up, and
7 decrypting the data originally backed up to obtain the actual data.

1 43. (Withdrawn) The method of claim 14, wherein the restoring of data from
2 the previously backed up data includes
3 retrieving previously backed up data from the backup partners until
4 sufficient previously backed up data is available for decoding, and
5 decrypting, decoding and decompressing all of the retrieved previously
6 backed up data.

1 44. (Original) The method of claim 1, wherein the data being backed up is
2 file contents.

1 45. (Currently Amended) A distributed cooperative backup system,
2 comprising:
3 a network; and
4 a loose confederation of computers connected via the network, a
5 plurality of computers from among the loose confederation of computers being
6 configured for distributed cooperative backing up of data, each computer of
7 the plurality of computers having a storage that can be used for providing
8 reciprocal backup services, and each computer of the plurality of computers
9 respectively having a computer readable medium embodying computer
10 program code configured to cause the computer to
11 form partnerships between the plurality of computers, each of the
12 partnerships being of computers such that each computer in a partnership
13 commits under an agreements to ~~help~~ store backup ~~the~~ data received from one

14 or more of its backup partners, whereby a first computer in each partnership
15 assumes the task of storing backup data received from one or more other
16 computers in the partnership and one or more of the other computers in the
17 partnership assume the task of storing backup data received from the first
18 computer;

19 back up data in accordance with the each agreements; and
20 periodically verify that previously backed up data is being retained by
21 the computers committed to act as backup partners in accordance with the
22 each agreements.

1 46. (Original) The system of claim 45, wherein each of the backup partners
2 may leave the system and return to the system at any time.

1 47. (Original) The system of claim 45, wherein prevention of freeloading is
2 enforced by the backup partners themselves, wherein any one of the backup
3 partners may be periodically requested to prove that it is retaining the
4 previously backed up data.

1 48. (Currently Amended) A distributed cooperative backup system,
2 comprising:

3 a network; and

4 a loose confederation of computers connected via the network, a
5 plurality of computers from among the loose confederation of computers being
6 configured for distributed cooperative backing up of data and functioning as
7 backup partners, each computer of the plurality of computers having a storage
8 that can be used for providing reciprocal backup services, and each computer
9 of the plurality of computers respectively having a computer readable medium
10 embodying computer program code configured to cause the computer to

11 select computers as potential backup partners from among the plurality
12 of computers based on predetermined criteria,

13 negotiate a reciprocal backup partnership agreement between the
14 computer and the selected computers based on predetermined requirements,
15 including backup requirements,

16 form partnerships between the computer and selected computers, the
17 computer and the selected computers becoming backup partners by agreeing to
18 cooperatively provide backup services to each other such that a first computer
19 in each partnership assumes the task of storing backup data received from one
20 or more other computers in the partnership and one or more of the other
21 computers in the partnership assume the task of storing backup data received
22 from the first computer and so that a distributed cooperative backing up of
23 data ~~can be~~ is administered in the absence of central control,
24 periodically back up data at the backup partners, encoding the data
25 each time before the data is backed up, and
26 periodically verify that previously backed up data is retained by the
27 backup partners.

1 49. (New) A method for backing up data on a plurality of computers
2 connected via a network, comprising:
3 exchanging messages among computers of the plurality to determine
4 the ability of each to satisfy backup storage requirements of one or more
5 others;
6 forming a partnership among computers of the plurality in which a first
7 computer in the partnership stores backup data received from one or more
8 other computers in the partnership and one or more of the other computers in
9 the partnership store backup data received from the first computer; and
10 each of the computers in the partnership periodically verifying that its
11 backup data is being retained by one or more of the other computers in the
12 partnership.

1 50. (New) The method according to claim 49, wherein the verifying includes
2 selecting a block of the previously backed up data wherein the selecting is not
3 controlled by any one of the computers individually.

1 51. (New) The method according to claim 49, wherein the partnership
2 consists of two computers.

1 52. (New) Computer readable media having stored thereon computer code
2 for a method of backing up data on a plurality of computers connected via a
3 network, the method comprising steps of:

4 exchanging messages among computers of the plurality to determine
5 the ability of each to satisfy backup storage requirements of one or more
6 others;

7 forming a partnership among computers of the plurality in which a first
8 computer in the partnership stores backup data received from one or more
9 other computers in the partnership and one or more of the other computers in
10 the partnership store backup data received from the first computer; and

11 periodically verifying that stored backup data is being retained by one
12 or more of the computers in the partnership.